

Jodi Golinsky
Vice President
Legislative/Regulatory & Privacy Counsel

MasterCard International
Law Department
2000 Purchase Street
Purchase, NY 10577-2509
914 249-5978
Fax 914 249-3648
E-mail jodi_golinsky@mastercard.com
www.mastercard.com

15

**MasterCard
International**



Via Electronic Delivery

October 14, 2003

Public Information Room
Office of the Comptroller of the Currency
250 E Street, SW, Mail Stop 1-5
Washington, DC 20219
ATTN: Docket No. 03-18

Email: regs.comments@occ.treas.gov

Ms. Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551

Email:
regs.comments@federalreserve.gov

Robert E. Feldman
Executive Secretary
ATTN: Comments/OES
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429

Email: comments@fdic.gov

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552
ATTN: No. 03-35

Email: regs.comments@ots.treas.gov

To whom it may concern:

This letter is submitted on behalf of MasterCard International Incorporated¹ ("MasterCard") in response to the proposed guidance entitled "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer

¹ MasterCard is a global membership organization comprised of financial institutions that are licensed to use the MasterCard service marks in connection with a variety of payments systems.

Notice" ("Proposal"). The Proposal is intended to interpret certain provisions of the Interagency Guidelines Establishing Standards for Safeguarding Customer Information ("Safeguarding Guidelines"). In particular, the Proposal describes the expectations of the federal banking agencies² ("Agencies") that every financial institution develop a response program to protect against and address reasonably foreseeable risks associated with internal and external threats to the security of customer information maintained by the financial institution or its service providers. MasterCard appreciates the opportunity to provide our comments on the Proposal.

In General

MasterCard believes that the Proposal offers useful guidance to financial institutions regarding how to develop appropriate response programs. The Agencies, in many instances, have provided reasonable objectives that should be met while allowing each financial institution the flexibility to determine how best to meet each objective. In other areas the Proposal is more prescriptive, such as provisions regarding the mitigation of harm to customers. We believe the Agencies have generally taken a reasonable, appropriate approach in these areas although, as discussed below, we suggest some modifications.

Scope of Application of Response Program

The Proposal indicates that the "Agencies expect every financial institution to develop a response program to protect against the risks associated with [reasonably foreseeable] threats" that "may lead to the misuse of customer information." The Supplementary Information to the Proposal further clarifies that it is "the Agencies' expectations that every financial institution develop a response program to protect against and address reasonably foreseeable risks associated with...threats to the security of customer information maintained by the financial institution or its service provider."

MasterCard supports the Agencies' determination that a financial institution's response program should be developed based on reasonably foreseeable risks. We believe this is an appropriate focus for a financial institution, allowing it to develop and implement a program based on what can reasonably be foreseen. Furthermore, this approach is consistent with the existing Safeguarding Guidelines which obligate a financial institution, as part of its risk assessment, to identify those risks that are reasonably foreseeable. Therefore, we urge the Agencies to adopt this approach in its final Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice ("Final Guidelines").

² The federal banking agencies include the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision.

Components of Response Program

Assess the Situation

The Proposal states that a response program should include a provision requiring the financial institution to assess the nature and scope of the incident, and identify the customer information systems and types of customer information that have been accessed or misused. This is clearly a key component of a response program and the Proposal allows flexibility for financial institutions to determine how to achieve it. We urge the Agencies to retain this approach in the Final Guidelines.

Notify Regulatory and Law Enforcement Agencies

The Proposal indicates that a financial institution should promptly notify its primary federal regulator when the institution becomes aware of an incident involving unauthorized access to or use of customer information that "could" result in substantial harm or inconvenience to its customers. MasterCard agrees that a financial institution should promptly notify its primary federal regulator of certain security breaches. We believe, however, that the Proposal should clarify that a financial institution must notify its primary federal regulator if the breach involves "sensitive" customer information ("SCI") that "poses a significant risk of substantial harm to a significant number of its customers." As a practical matter, it appears unlikely that a breach that involves customer information that is not SCI would pose a significant risk of substantial harm to its customers. Indeed, the Proposal's customer notification obligations appear to be predicated on the notion that substantial customer harm or inconvenience is likely to result only if customer information that is SCI is improperly accessed and/or used. In addition, notice should not be required merely because a breach "could" involve customer harm. Instead, the notification to regulators should be required when it is determined that the breach, in fact, "poses a significant risk" of the customer harms covered by the Proposal. These two clarifications of the reporting requirement will allow institutions to better discern when it is appropriate to notify primary federal regulators. They will also reduce the number of reports sent unnecessarily to the Agencies, thereby conserving the information security resources of the institutions and the Agencies alike.

Contain and Control the Situation

Under the Proposal, a financial institution would be expected to take measures to contain and control an incident to prevent further unauthorized access to, or use of, customer information while preserving records and other evidence. The Proposal also provides several measures that could be used to contain and control the situation. Importantly, the Proposal takes the approach of establishing a goal to be achieved while giving financial institutions flexibility to achieve that goal "[d]epending upon the particular facts and circumstances of the incident." We urge the Agencies to retain this general approach in the Final Guidelines.

Corrective Measures

The Proposal states that once an institution understands the scope of the incident, and has taken steps to contain and control the situation, it should take measures to address and mitigate the harm to individual customers. We appreciate the recognition of the fact that the appropriate corrective measures cannot be taken until an institution understands the scope of the incident and takes steps to contain and control the situation. We believe the Proposal sets the proper priorities with respect to an institution's obligations, and this approach should be retained in the Final Guidelines.

As part of a financial institution's corrective measures, the Proposal indicates that the institution should take certain measures, including flagging accounts, securing accounts, and providing customer notice and assistance. We suggest that the Agencies clarify that a financial institution should take such measures "when appropriate." For example, it appears that providing customers with a notice of the incident is not required by the Proposal in all instances, only a portion of those involving unauthorized access to SCI.

Flag Accounts

According to the Proposal, the institution should identify and monitor the accounts of those customers whose information may have been accessed or misused. MasterCard believes this is a prudent measure that protects customers, as well as the institution itself. However, we believe that an institution should be obligated to flag accounts only if the facts and circumstances suggest that the accounts may be compromised. For example, it seems unnecessary to flag accounts if the information accessed was aggregated or otherwise could not be used to harm customers.

Secure Accounts

The Agencies state that if "a checking, savings, or other deposit account number, debit or credit card account number, personal identification number (PIN), password, or other unique identifier has been accessed or misused, the financial institution should secure the account." The Proposal provides no guidance with respect to what is meant by securing an account. We believe that the Final Guidelines should give the institution flexibility to take appropriate steps to protect the account from misuse and the customer against harm. Depending on the facts and circumstances of the situation, and depending on the sophistication of the institution, this could involve a variety of precautions, such as changing an internal password or adding a PIN to the account. We urge the Agencies to provide this clarification in the Final Guidelines.

MasterCard is also concerned that, under the Proposal, an account must be made "secure" "until such time as the financial institution and the customer agree on a course of action." We believe that the more appropriate obligation for a financial institution is to take appropriate measures to protect the account from misuse, and the customer from

harm. This achieves the underlying objectives of the Proposal while allowing the financial institution to evaluate the particular facts and circumstances of the security breach.

In any event, the Proposal should avoid the suggestion that the financial institution must come to an agreement with each and every affected customer with respect to how an account that is the subject of unauthorized access is to be handled. As a primary matter, the Proposal does not require customer notification except when SCI is accessed without authorization, and only then in certain circumstances. Furthermore, it may be that unauthorized access to unique identifiers to an account can be remedied without needing to communicate with the customer—such as if the financial institution has controls in place to ensure that the compromised information cannot be used in a harmful manner. We are also concerned that a financial institution must “agree” to various courses of action with customers. For example, if thousands of account numbers were misused, a card issuer may determine that the most appropriate course of action is to notify the affected cardholders and to convert the compromised accounts to new accounts with reissued cards. The card issuer should not be expected to contact thousands of cardholders to verify that they each individually agree to such a course of action. Indeed, customers would suffer severe inconvenience if swift, protective action could not be taken as a result of an obligation to obtain agreement from thousands of customers.

Customer Notice and Assistance: Circumstances under which Notice Must Be Given

A financial institution must notify and offer assistance to a customer if the institution is aware that a customer’s SCI has been accessed improperly unless the institution, after an appropriate investigation, reasonably concludes that misuse of the SCI is unlikely to occur and takes steps to safeguard the interests of the affected customer. For purposes of the Proposal, SCI means “a customer’s social security number, [PIN], password or account number, in conjunction with a personal identifier such as the customer’s name, address, or telephone number.” SCI also includes any combination of components of customer information that would allow someone to log onto or access another person’s account, such as username and password.

We agree with the Agencies’ approach of limiting a financial institution’s notice obligation to certain circumstances. However, we believe that the standard used to trigger notice to customers should be more precisely defined. Specifically, we believe that an institution should be required to notify affected customers when it becomes aware of unauthorized access to SCI under its control unless the institution reasonably concludes that misuse of the information is unlikely to occur, or the burden of notification on the customer and the institution outweighs the value of individual customer notification. If an institution concludes that a notice to its customers is not required, the institution may nevertheless be required to take appropriate steps to protect the affected customers and the institution, including, where appropriate, monitoring affected customers’ accounts for unusual or suspicious activity.

The Proposal includes a definition of SCI which, as a general matter, will provide financial institutions with helpful guidance in their efforts to comply with the Final Guidelines. We believe, however, that further clarifications are necessary to avoid potential confusion in certain areas. First, we do not believe that encrypted information should be considered SCI. Therefore, SCI should apply only to *unencrypted* data elements covered by the Proposal. Second, the Proposal indicates that one data element of SCI would be the customer's name. We urge the Agencies to clarify that the data element is the customer's first name (or first initial) and last name. Third, it should be clarified that an account number alone should not be deemed to be SCI unless it is combined with other information that would enable access to a customer's financial account. In this regard, an account number alone may not be used in ways harmful to consumers unless it is combined with other information that permits access to a customer's account.

Although a "bright line" test is appropriate with respect to the definition of SCI, MasterCard believes the flexibility must be provided with respect to when a notice must be sent after SCI is subject to unauthorized access. Specifically, the Final Guidelines should incorporate the important balancing test described above with respect to customer notices. In particular, the notices should be sent only if their benefits exceed their burdens on customers and financial institutions. Customers should not receive notices that will potentially cause personal concern and anxiety unless it is appropriate based on the circumstances.

The Proposal states that if an institution can determine which customers' information was accessed or misused, it may restrict notification to those individuals. We believe this obligation is reasonable and should be retained in the Final Guidelines. The Proposal also states, however, that if the institution cannot identify precisely which customers are affected, it should notify each customer in "groups" likely to have been affected, "such as each customer whose information is stored in the group of files in question." MasterCard is concerned that such a requirement could unintentionally create confusion whether a database containing millions of customer records might be the relevant "group" even though only a portion of the customers in the database are likely to be affected. In order to avoid such confusion we suggest that the provision be modified to make it clear that where the institution cannot identify precisely which customers are affected it should notify the groups likely to have been affected, "such as each customer *likely to have been affected* whose information is stored in the group of files in question."

The Proposal states that the required notice "should be timely, clear, and conspicuous, and delivered in any manner that will ensure that the customer is likely to receive it." MasterCard believes that these standards are generally appropriate. However, we believe the Agencies should clarify that a financial institution may delay sending notices to customers if the institution is notified by law enforcement or the appropriate federal regulator that sending a notice to customers may impede an ongoing investigation. We also believe that a financial institution should be permitted additional time to send the notice if sending the notice would impede an internal investigation of the security breach. Apprehension of the criminal intruder(s) should be a key priority, especially because an

arrest of the criminal(s) will also help ensure they are not able to misuse customer data any further.

MasterCard notes that the Final Guidelines should also include alternative notice options for a financial institution in certain circumstances. For example, if providing the notice to customers would cost more than \$250,000, or if the affected class of persons to be notified exceeds 500,000, the financial institution should be given the alternative of notifying major media outlets in markets with significant numbers of affected customers. Such a notification will meet the objectives of the Proposal (*i.e.* to provide meaningful notice to customers) without imposing undue hardship on the financial institution.

Customer Notice and Assistance: How to Provide Notice

The Proposal suggests that a financial institution may provide the notice by telephone or by mail. We applaud the Agencies for allowing the notice to be given using either one of these mechanisms. The Proposal suggests, however, that an electronic notice is only appropriate for "those customers who conduct transactions electronically." We understand the need to ensure that electronic notices are not used inappropriately but are concerned that the Proposal's approach may be too narrow. Indeed, some customers may exchange communications with a financial institution electronically even if they do not "conduct transactions electronically." To address this issue, electronic notice should suffice if the customer conducts transactions electronically or the institution has met its relevant obligations under the federal E-SIGN Act.

We also urge the Agencies to provide clarification that a telephone call made to a customer for purposes of complying with the Proposal will be deemed to be for "emergency purposes." This is an important clarification in light of certain issues which may be raised under the Telephone Consumer Protection Act ("TCPA") and its implementing regulations. In particular, the Federal Communications Commission has stated that it is unlawful to make any call using an automatic telephone dialing system or a prerecorded message to any wireless telephone number unless such call is for "emergency purposes." We believe that a financial institution would have just cause to use such mechanisms to deliver notices to customers as expeditiously as possible. In many instances, for example, automated telephone calls can be made in less time than it takes to deliver mail. However, it is likely that some telephone numbers provided by customers for contact purposes are wireless numbers. Financial institutions may be discouraged from making certain types of telephone calls to customers to notify them of a security breach, and therefore use mechanisms that do not provide notice as quickly to customers, unless they receive clarification that such calls are for "emergency purposes."

Customer Notice and Assistance: Contents of Notice

The Proposal describes what a financial institution should include in the contents of the notice. For example, the notice should describe the incident in general terms and the customer's information that was the subject of unauthorized access or use. We agree that the financial institution should provide a general description of the reasons the customer is

receiving a notice. A financial institution should be given the option, however, of stating the *types* of information that *may* be the subject of unauthorized access or use. For example, it should be sufficient to note that the customer's name and social security number may have been accessed without having to print the customer's social security number on the notice. Furthermore, it may not always be clear to the institution what information has been accessed or used with respect to an individual customer.

Under the Proposal, the financial institution would also be required to inform the customer that the institution will assist the customer to correct and update information in any credit report relating to the customer as required by the Fair Credit Reporting Act. MasterCard urges the Agencies to clarify this obligation so that the customer has a better and more accurate understanding of how the financial institution may be able to assist the customer. In particular, the financial institution should not be required to include this information unless the breach is likely to result in the financial institution furnishing inaccurate data to a credit bureau. Furthermore, the financial institution should be permitted to specify that it will assist the customer to correct and update information, as appropriate, that the financial institution reported to the credit bureau. In this regard, the customer should not be led to expect that the breach will necessarily result in errors on the customer's credit report or that the financial institution can assist with the correction of information the financial institution did not provide.

The Proposal also requires a financial institution to recommend that the customer place a fraud alert in the customer's credit reports. Although a customer may determine that placing a fraud alert in his or her file at a credit bureau is appropriate, we do not believe that the financial institution should issue a blanket recommendation that every customer take such precaution. For example, the information compromised may not be sufficient to affect the customer's credit report. This would be especially true if the financial institution took appropriate action to render the compromised information worthless. Furthermore, a customer may determine that the consequences of a fraud alert, such as increased obstacles in obtaining credit, outweigh any potential benefit. Thus, we do not believe it to be appropriate for the financial institution to make such a blanket recommendation. If the Agencies determine that the notice should discuss fraud alerts, we believe the discussion should be limited to the fact that the customer may choose to have one inserted in his or her credit file.

The Proposal also provides that the notice furnished to a customer must inform the customer of the right to obtain a credit report free of charge if the customer has reason to believe that the file at the credit bureau contains inaccurate information due to fraud. We urge the Agencies to modify this requirement. As a factual matter, the customer may *not* have a right to a free credit report under such circumstances if the customer, during the previous 12 months, has already obtained a free credit report on account of such belief. If the Agencies choose to require that the financial institution provide the customer with information pertaining to a free credit report, MasterCard suggests that the Proposal be amended to require the financial institution to inform the customer that the customer *may* have the ability under federal or state law to obtain a credit report free of charge.

The Proposal suggests several optional elements the financial institution could include in its notice to a customer. These include providing a toll-free telephone number that customers can call for assistance, offering to assist the customer in notifying nationwide credit bureaus, and informing the customer about credit report subscription services. Although we agree with the Agencies that such elements should not be required in the notice provided to customers, we urge the Agencies to delete the reference to optional components. By providing a list of optional elements, the Agencies are suggesting that other elements would not be appropriate or useful. We believe it would be better for the Agencies to include in the Final Guidelines what is expected to be included in the notice and allow financial institutions the ability to include other provisions as they deem necessary or useful.

Customer Notice and Assistance: Appropriately Trained Employees

As part of the financial institution's obligation to notify and provide assistance to certain customers, a footnote in the Proposal suggests that the "institution should, therefore, ensure that a sufficient number of appropriately trained employees are available to answer customer inquiries and provide assistance." Although MasterCard believes that it is reasonable for a financial institution to field customer service calls generated as a result of security breaches, it is unreasonable to expect a financial institution to have "a sufficient number of appropriately trained employees" for any possible circumstance, such as those involving potentially massive short-term surges in customer service inquiries. For example, in a worst-case scenario, if a financial institution had to notify millions of customers of a security breach, it is reasonable to assume that the inbound customer calls to the financial institution will spike to unpredictable levels. It simply may not be possible to have a "sufficient" number of people available to ensure customer calls are answered without requiring the customer to remain on hold for a period of time. We believe a more appropriate requirement would be for the financial institution to have reasonable procedures in place, taking into account the institution's size and employee base, to respond appropriately to customer inquiries and requests for assistance.

Service Providers

The Proposal states that "[c]onsistent with existing guidance issued by the Agencies, an institution's contract with its service provider should require the service provider to fully disclose to the institution information relating to any breach in security resulting in an unauthorized intrusion into the institution's customer information systems maintained by the service provider." MasterCard agrees that financial institutions should include such provisions, as appropriate, in contracts with service providers. Indeed, it is the service provider's obligation to inform the financial institution of any security breach involving the financial institution's customer data. This approach should be retained in the Final Guidelines.

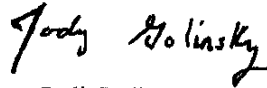
* * * * *

October 14, 2003

Page 10

If you have any questions concerning our comments, or if we may otherwise be of assistance in connection with this issue, please do not hesitate to call me, at the number indicated above, or Michael F. McEneney at Sidley Austin Brown & Wood LLP, at (202) 736-8368, our counsel in connection with this matter.

Sincerely,

A handwritten signature in black ink that reads "Jodi Golinsky". The signature is written in a cursive, flowing style.

Jodi Golinsky
Vice President
Legislative/Regulatory & Privacy Counsel

cc: Michael F. McEneney, Esq.